

# Normal bases for modular function fields

JA KYUNG KOO, DONG HWA SHIN AND DONG SUNG YOON\*

## Abstract

We provide a concrete example of a normal basis for a finite Galois extension which is not abelian. More precisely, let  $\mathbb{C}(X(N))$  be the field of meromorphic functions on the modular curve  $X(N)$  of level  $N$ . We construct a completely free element in the extension  $\mathbb{C}(X(N))/\mathbb{C}(X(1))$  by means of Siegel functions.

## 1 Introduction

Let  $E$  be a finite Galois extension of a field  $F$  with

$$G = \text{Gal}(E/F) = \{\sigma_1, \sigma_2, \dots, \sigma_n\}.$$

The well-known normal basis theorem ([12]) states that there always exists an element  $a$  of  $E$  for which

$$\{a^{\sigma_1}, a^{\sigma_2}, \dots, a^{\sigma_n}\}$$

becomes a basis for  $E$  over  $F$ . We call such a basis a *normal basis* for the extension  $E/F$ , and say that the element  $a$  is *free* in  $E/F$ . In other words,  $E$  is a free  $F[G]$ -module of rank 1 generated by  $a$ . Moreover, Blessenohl and Johnson proved in [1] that there is a primitive element  $a$  for  $E/F$  which is free in  $E/L$  for every intermediate field  $L$  of  $E/F$ . Such an element  $a$  is said to be *completely free* in the extension  $E/F$ . However, not much is known so far about explicit construction of (completely) free elements when  $F$  is infinite. As for number fields, we refer to [2], [3], [5], [7], [8], [9], [11].

For a positive integer  $N$ , let

$$\Gamma(N) = \{\sigma \in \text{SL}_2(\mathbb{Z}) \mid \sigma \equiv I_2 \pmod{N \cdot M_2(\mathbb{Z})}\}$$

be the principal congruence subgroup of  $\text{SL}_2(\mathbb{Z})$  of level  $N$  which acts on the upper half-plane  $\mathbb{H} = \{\tau \in \mathbb{C} \mid \text{Im}(\tau) > 0\}$  by fractional linear transformations. Corresponding to  $\Gamma(N)$ , let

$$X(N) = \Gamma(N) \backslash \mathbb{H}^*$$

be the modular curve of level  $N$ , where  $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$  ([10, Chapter 1]). We denote its meromorphic function fields by  $\mathbb{C}(X(N))$ . As is well known,  $\mathbb{C}(X(N))$  is a Galois extension of  $\mathbb{C}(X(1))$  with

$$\text{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \simeq \Gamma(1)/\pm \Gamma(N) \simeq \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} \quad (1)$$

---

2010 *Mathematics Subject Classification.* Primary 11F03, Secondary 11G16.

*Key words and phrases.* modular functions, modular units, normal bases

\*Corresponding author.

The second named author was supported by Hankuk University of Foreign Studies Research Fund of 2016.

([6, Theorem 2 in Chapter 6] and [10, Proposition 6.1]). Furthermore, if  $N \geq 2$ , then  $\mathbb{C}(X(N))$  is not an abelian extension of  $\mathbb{C}(X(1))$ . In this paper, we shall find a completely free element  $g(\tau)$  in  $\mathbb{C}(X(N))/\mathbb{C}(X(1))$  in terms of Siegel functions (Theorem 3.3). This gives a concrete example of a normal basis for a nonabelian Galois extension.

## 2 Siegel functions as modular functions

We shall briefly introduce Siegel functions and their basic properties, and further develop a couple of lemmas for later use.

For a lattice  $\Lambda$  in  $\mathbb{C}$ , the *Weierstrass  $\sigma$ -function* relative to  $\Lambda$  is defined by

$$\sigma(z; \Lambda) = z \prod_{\lambda \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{\lambda}\right) e^{z/\lambda + (1/2)(z/\lambda)^2} \quad (z \in \mathbb{C}).$$

Taking logarithmic derivative, we obtain the *Weierstrass  $\zeta$ -function*

$$\zeta(z; \Lambda) = \frac{\sigma'(z; \Lambda)}{\sigma(z; \Lambda)} = \frac{1}{z} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left( \frac{1}{z - \lambda} + \frac{1}{\lambda} + \frac{z}{\lambda^2} \right) \quad (z \in \mathbb{C}).$$

One can readily see that

$$\zeta'(z; \Lambda) = -\frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left( -\frac{1}{(z - \lambda)^2} + \frac{1}{\lambda^2} \right),$$

which is periodic with respect to  $\Lambda$ . Thus, for each  $\lambda \in \Lambda$ , there is a constant  $\eta(\lambda; \Lambda)$  such that

$$\zeta(z + \lambda; \Lambda) - \zeta(z; \Lambda) = \eta(\lambda; \Lambda) \quad (z \in \mathbb{C}).$$

Now, for  $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ , we define the *Siegel function*  $g_{\mathbf{v}}(\tau)$  by

$$g_{\mathbf{v}}(\tau) = \exp(-(1/2)(v_1\eta(\tau; [\tau, 1]) + v_2\eta(1; [\tau, 1]))(v_1\tau + v_2)) \sigma(v_1\tau + v_2; [\tau, 1])\eta(\tau)^2 \quad (\tau \in \mathbb{H}),$$

where  $[\tau, 1] = \tau\mathbb{Z} + \mathbb{Z}$  and  $\eta(\tau)$  is the *Dedekind  $\eta$ -function* given by

$$\eta(\tau) = \sqrt{2\pi} e^{\pi i/4} q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \quad (q = e^{2\pi i\tau}, \tau \in \mathbb{H}). \quad (2)$$

Let

$$\mathbf{B}_2(x) = x^2 - x + \frac{1}{6} \quad (x \in \mathbb{R})$$

be the second Bernoulli polynomial, and let  $\langle x \rangle$  be the fractional part of  $x$  in the interval  $[0, 1)$ .

**PROPOSITION 2.1.** *Let  $\mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \in (1/N)\mathbb{Z}^2 \setminus \mathbb{Z}^2$  for an integer  $N \geq 2$ .*

(i)  *$g_{\mathbf{v}}(\tau)$  has the infinite product expansion*

$$g_{\mathbf{v}}(\tau) = -e^{\pi i v_2(v_1-1)} q^{(1/2)\mathbf{B}_2(v_1)} (1 - q^{v_1} e^{2\pi i v_2}) \prod_{n=1}^{\infty} (1 - q^{n+v_1} e^{2\pi i v_2}) (1 - q^{n-v_1} e^{-2\pi i v_2})$$

*with respect to  $q = e^{2\pi i\tau}$ .*

(ii) We have the  $q$ -order formula

$$\text{ord}_q g_{\mathbf{v}}(\tau) = \frac{1}{2} \mathbf{B}_2(\langle v_1 \rangle).$$

(iii)  $g_{\mathbf{v}}(\tau)^{12N}$  belongs to  $\mathbb{C}(X(N))$  and has neither zeros nor poles on  $\mathbb{H}$ .

(iv)  $g_{\mathbf{v}}(\tau)^{12N}$  depends only on  $\pm \mathbf{v} \pmod{\mathbb{Z}^2}$ , and satisfies

$$(g_{\mathbf{v}}(\tau)^{12N})^{\sigma} = (g_{\mathbf{v}}^{12N} \circ \sigma)(\tau) = g_{\sigma^T \mathbf{v}}(\tau)^{12N} \quad (\sigma \in \text{SL}_2(\mathbb{Z})),$$

where  $\sigma^T$  stands for the transpose of  $\sigma$ .

PROOF. (i) See [4, K 4 in p. 29].

(ii) See [4, p. 31].

(iii) See [4, Theorem 1.2 in Chapter 2].

(iv) See [4, Proposition 1.3 in Chapter 2].

□

For a positive integer  $N$ , let  $\Gamma_1(N)$  be the congruence subgroup of  $\text{SL}_2(\mathbb{Z})$  defined by

$$\Gamma_1(N) = \left\{ \sigma \in \text{SL}_2(\mathbb{Z}) \mid \sigma \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N \cdot M_2(\mathbb{Z})} \right\}.$$

Now, we let  $N \geq 2$ , and consider the function

$$g(\tau) = g_{\begin{bmatrix} 0 \\ 1/N \end{bmatrix}}(\tau)^{-12N\ell} g_{\begin{bmatrix} 1/N \\ 0 \end{bmatrix}}(\tau)^{-12Nm}$$

where  $\ell$  and  $m$  are integers such that  $\ell > m > 0$ . Then we see from Proposition 2.1 (iii) that  $g(\tau)$  belongs to  $\mathbb{C}(X(N))$ .

LEMMA 2.2. We have

$$\text{ord}_q \left( \frac{g(\tau)^{\sigma}}{g(\tau)} \right) \geq 0 \quad \text{for all } \sigma \in \text{SL}_2(\mathbb{Z}).$$

The equality holds if and only if  $\sigma \in \pm \Gamma_1(N)$ .

PROOF. Let  $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z})$ . Note that  $a \equiv c \equiv 0 \pmod{N}$  is impossible. We get by Proposition 2.1 (iv) and (ii) that

$$\begin{aligned} \text{ord}_q \left( \frac{g(\tau)^{\sigma}}{g(\tau)} \right) &= \text{ord}_q \left( \frac{g_{\begin{bmatrix} c/N \\ d/N \end{bmatrix}}(\tau)^{-12N\ell} g_{\begin{bmatrix} a/N \\ b/N \end{bmatrix}}(\tau)^{-12Nm}}{g_{\begin{bmatrix} 0 \\ 1/N \end{bmatrix}}(\tau)^{-12N\ell} g_{\begin{bmatrix} 1/N \\ 0 \end{bmatrix}}(\tau)^{-12Nm}} \right) \\ &= 6N (\ell \mathbf{B}_2(0) + m \mathbf{B}_2(1/N) - \ell \mathbf{B}_2(\langle c/N \rangle) - m \mathbf{B}_2(\langle a/N \rangle)). \end{aligned}$$

Then we deduce from the fact  $\ell > m > 0$  and Figure 1 that

$$\text{ord}_q \left( \frac{g(\tau)^{\sigma}}{g(\tau)} \right) \geq 0$$

with equality if and only if

$$\langle c/N \rangle = 0 \quad \text{and} \quad \langle a/N \rangle = 1/N \text{ or } 1 - 1/N. \quad (3)$$

Moreover, by the relation  $\det(\sigma) = ad - bc = 1$  one can express the condition (3) as

$$\sigma \equiv \pm \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N \cdot M_2(\mathbb{Z})}.$$

This proves the lemma. □

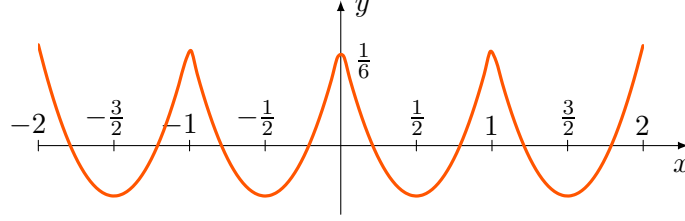


Figure 1: The graph of  $y = \mathbf{B}_2(\langle x \rangle)$

Let  $\mathbb{R}_+$  denote the set of positive real numbers.

LEMMA 2.3. *Given any  $\varepsilon \in \mathbb{R}_+$ , we can take  $r \in \mathbb{R}_+$  and an integer  $m$  large enough so that*

$$\left| \frac{g^\sigma(r\mathbf{i})}{g(r\mathbf{i})} \right| < \varepsilon \quad \text{for all } \sigma \in \mathrm{SL}_2(\mathbb{Z}) \setminus \pm\Gamma(N).$$

PROOF. First, consider the case where  $\sigma \notin \pm\Gamma_1(N)$ . Then, we obtain by Lemma 2.2 that

$$\mathrm{ord}_q \left( \frac{g(\tau)^\sigma}{g(\tau)} \right) > 0,$$

which implies that  $g(\tau)^\sigma/g(\tau)$  has a zero at the cusp  $\mathbf{i}\infty$ . Hence we can take  $r_\sigma \in \mathbb{R}_+$  sufficiently large so as to have

$$\left| \frac{g^\sigma(r_\sigma \mathbf{i})}{g(r_\sigma \mathbf{i})} \right| < \varepsilon.$$

Set

$$r = \max \{ r_\sigma \mid \sigma \in \mathrm{SL}_2(\mathbb{Z}) \setminus \pm\Gamma_1(N) \}.$$

Second, let  $\sigma \in \pm\Gamma_1(N) \setminus \pm\Gamma(N)$ , and so  $\sigma \equiv \pm \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \pmod{N \cdot M_2(\mathbb{Z})}$  for some  $b \in \mathbb{Z}$  with  $b \not\equiv 0 \pmod{N}$ . We then derive that

$$\begin{aligned} \left| \frac{g^\sigma(r\mathbf{i})}{g(r\mathbf{i})} \right| &= \left| \frac{g \begin{bmatrix} 0 & \\ 1/N & \end{bmatrix} (r\mathbf{i})^{-12N\ell} g \begin{bmatrix} 1/N & \\ b/N & \end{bmatrix} (r\mathbf{i})^{-12Nm}}{g \begin{bmatrix} 0 & \\ 1/N & \end{bmatrix} (r\mathbf{i})^{-12N\ell} g \begin{bmatrix} 1/N & \\ 0 & \end{bmatrix} (r\mathbf{i})^{-12Nm}} \right| \quad \text{by Proposition 2.1 (iv)} \\ &= \left| \frac{g \begin{bmatrix} 1/N & \\ 0 & \end{bmatrix} (r\mathbf{i})^{12Nm}}{g \begin{bmatrix} 1/N & \\ b/N & \end{bmatrix} (r\mathbf{i})^{12Nm}} \right| \\ &= \left| \frac{1 - R^{1/N}}{1 - R^{1/N} \zeta_N^b} \right|^{12Nm} \prod_{n=1}^{\infty} \left| \frac{(1 - R^{n+1/N})(1 - R^{n-1/N})}{(1 - R^{n+1/N} \zeta_N^b)(1 - R^{n-1/N} \zeta_N^{-b})} \right|^{12Nm} \\ &\quad \text{by Proposition 2.1 (i), where } R = e^{-2\pi r} \text{ and } \zeta_N = e^{2\pi \mathbf{i}/N} \end{aligned}$$

$$\leq \left| \frac{1 - R^{1/N}}{1 - R^{1/N} \zeta_N^b} \right|^{12Nm}$$

because  $|1 - x| \leq |1 - x\zeta|$  for any  $x \in \mathbb{R}_+$  with  $x < 1$  and any root of unity  $\zeta$ .

Therefore, if  $m$  is sufficiently large, then we attain

$$\left| \frac{g^\sigma(ri)}{g(ri)} \right| < \varepsilon.$$

This completes the proof. □

### 3 Completely free elements in modular function fields

Let  $N \geq 2$ . In this section, we shall show that

$$g(\tau) = g_{\begin{bmatrix} 0 & \\ 1/N & \end{bmatrix}}(\tau)^{-12N\ell} g_{\begin{bmatrix} 1/N & \\ 0 & \end{bmatrix}}(\tau)^{-12Nm} \quad \text{with } \ell > m > 0$$

plays an important role as completely normal elements in modular function field extensions.

PROPOSITION 3.1. *The function  $g(\tau)$  generates  $\mathbb{C}(X(N))$  over  $\mathbb{C}(X(1))$ .*

PROOF. Suppose that  $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z})$  leaves  $g(\tau)$  fixed. In particular, since  $\text{ord}_q g(\tau) = \text{ord}_q g(\tau)^\sigma$ , we get by Lemma 2.2 that  $\sigma \in \pm\Gamma_1(N)$ . Furthermore, we see by Proposition 2.1 (iv) and (ii) that

$$\begin{aligned} \text{ord}_q g(\tau)^{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}} &= \text{ord}_q \left( g_{\begin{bmatrix} 1/N & \\ 0 & \end{bmatrix}}(\tau)^{-12N\ell} g_{\begin{bmatrix} 0 & \\ -1/N & \end{bmatrix}}(\tau)^{-12Nm} \right) \\ &= -6N\ell \mathbf{B}_2(1/N) - 6Nm \mathbf{B}_2(0) \\ &= \text{ord}_q (g(\tau)^\sigma)^{\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}} \\ &= \text{ord}_q g(\tau)^{\begin{bmatrix} b & -a \\ d & -c \end{bmatrix}} \\ &= \text{ord}_q \left( g_{\begin{bmatrix} d/N & \\ -c/N & \end{bmatrix}}(\tau)^{-12N\ell} g_{\begin{bmatrix} b/N & \\ -a/N & \end{bmatrix}}(\tau)^{-12Nm} \right) \\ &= -6N\ell \mathbf{B}_2(\langle d/N \rangle) - 6Nm \mathbf{B}_2(\langle b/N \rangle). \end{aligned}$$

Thus we obtain  $b \equiv 0 \pmod{N}$ , and hence  $\sigma \in \pm\Gamma(N)$ . Therefore, we conclude by (1) and the Galois theory that  $g(\tau)$  generates  $\mathbb{C}(X(N))$  over  $\mathbb{C}(X(1))$ . □

THEOREM 3.2. *Let  $X^0(N)$  be the modular curve for the congruence subgroup*

$$\Gamma^0(N) = \left\{ \sigma \in \text{SL}_2(\mathbb{Z}) \mid \sigma \equiv \begin{bmatrix} * & 0 \\ * & * \end{bmatrix} \pmod{N \cdot M_2(\mathbb{Z})} \right\}$$

*with meromorphic function field  $\mathbb{C}(X^0(N))$ . Then,  $g(\tau)$  is completely free in  $\mathbb{C}(X(N))/\mathbb{C}(X^0(N))$ .*

PROOF. Note that  $\mathbb{C}(X(N))$  is a Galois extension of  $\mathbb{C}(X^0(N))$  with

$$\text{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X^0(N))) \simeq \Gamma^0(N)/\pm\Gamma(N).$$

It follows from Proposition 3.1 that  $g(\tau)$  generates  $\mathbb{C}(X(N))$  over  $\mathbb{C}(X^0(N))$ .

Now, let  $L$  be any intermediate field of  $\mathbb{C}(X(N))/\mathbb{C}(X^0(N))$  with

$$\text{Gal}(\mathbb{C}(X(N))/L) = \{\sigma_1 = \text{Id}, \sigma_2, \dots, \sigma_k\}.$$

Since  $\Gamma^0(N) \cap \pm\Gamma_1(N) = \pm\Gamma(N)$ , we must have

$$\sigma_i \notin \pm\Gamma_1(N) \quad (i = 2, \dots, k). \quad (4)$$

Set

$$g_i = g(\tau)^{\sigma_i} \quad (i = 1, 2, \dots, k),$$

and suppose that

$$c_1 g_1 + c_2 g_2 + \dots + c_k g_k = 0 \quad \text{for some } c_1, c_2, \dots, c_k \in L. \quad (5)$$

Acting each  $\sigma_i$  ( $i = 1, 2, \dots, k$ ) on both sides of (5) we achieve the system of equations

$$\begin{cases} c_1 g_1^{\sigma_1} + c_2 g_2^{\sigma_1} + \dots + c_k g_k^{\sigma_1} &= 0, \\ c_1 g_1^{\sigma_2} + c_2 g_2^{\sigma_2} + \dots + c_k g_k^{\sigma_2} &= 0, \\ &\vdots \\ c_1 g_1^{\sigma_k} + c_2 g_2^{\sigma_k} + \dots + c_k g_k^{\sigma_k} &= 0, \end{cases}$$

which can be rewritten as

$$A \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad \text{with } A = [g_j^{\sigma_i}]_{1 \leq i, j \leq k}.$$

Letting  $S_k$  be the permutation group on  $\{1, 2, \dots, k\}$ , we derive that

$$\begin{aligned} \det(A) &= \sum_{j_1 j_2 \dots j_k \in S_k} \text{sgn}(j_1 j_2 \dots j_k) g_{j_1}^{\sigma_1} g_{j_2}^{\sigma_2} \dots g_{j_k}^{\sigma_k} \\ &= \pm g^k + \sum_{\substack{j_1 j_2 \dots j_k \in S_k \text{ such that} \\ \sigma_{j_1} \sigma_{j_2} \dots \sigma_{j_k} \neq \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_k^{-1}}} \pm g^{\sigma_{j_1} \sigma_1} g^{\sigma_{j_2} \sigma_2} \dots g^{\sigma_{j_k} \sigma_k} \\ &= \pm g^k \left( 1 + \sum_{\substack{j_1 j_2 \dots j_k \in S_k \text{ such that} \\ \sigma_{j_1} \sigma_{j_2} \dots \sigma_{j_k} \neq \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_k^{-1}}} \pm \left( \frac{g^{\sigma_{j_1} \sigma_1}}{g} \right) \left( \frac{g^{\sigma_{j_2} \sigma_2}}{g} \right) \dots \left( \frac{g^{\sigma_{j_k} \sigma_k}}{g} \right) \right). \end{aligned}$$

Observe that for each  $j_1 j_2 \dots j_k \in S_k$  with  $\sigma_{j_1} \sigma_{j_2} \dots \sigma_{j_k} \neq \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_k^{-1}$ , we have

$$\sigma_{j_i} \sigma_i \neq \text{Id} \quad \text{for some } 1 \leq i \leq k.$$

Thus we attain that

$$\begin{aligned} \text{ord}_q \det(A) &= \text{ord}_q g^k \quad \text{by (4) and Lemma 2.2} \\ &= -6kN (\ell \mathbf{B}_2(0) + m \mathbf{B}_2(1/N)) \quad \text{by Proposition 2.1 (ii)} \\ &< 0 \quad \text{by the fact } \ell > m > 0 \text{ and Figure 1,} \end{aligned}$$

which implies that

$$\det(A) \neq 0 \quad \text{and} \quad c_1 = c_2 = \dots = c_k = 0.$$

Therefore,  $\{g_1, g_2, \dots, g_k\}$  is linearly independent over  $L$ ; and hence  $g(\tau)$  is completely free in  $\mathbb{C}(X(N))/\mathbb{C}(X^0(N))$ .  $\square$

THEOREM 3.3. *There is a positive integer  $M$  for which*

$$g(\tau) = g_{\begin{bmatrix} 0 \\ 1/N \end{bmatrix}}(\tau)^{-12N\ell} g_{\begin{bmatrix} 1/N \\ 0 \end{bmatrix}}(\tau)^{-12Nm}$$

*is completely free in  $\mathbb{C}(X(N))/\mathbb{C}(X(1))$  for  $\ell > m > M$ .*

PROOF. Let  $d = [\mathbb{C}(X(N)) : \mathbb{C}(X(1))]$ . We see from Lemma 2.3 and (1) that there exist a positive integer  $M$  and  $r \in \mathbb{R}_+$  so that if  $\ell > m > M$ , then

$$\left| \frac{g^\sigma(r\mathbf{i})}{g(r\mathbf{i})} \right| < \frac{1}{d! - 1} \quad \text{for all } \sigma \in \text{Gal}(\mathbb{C}(X(N))/\mathbb{C}(X(1))) \text{ with } \sigma \neq \text{Id}. \quad (6)$$

Now, let  $\ell > m > M$ . Let  $L$  be any intermediate field of  $\mathbb{C}(X(N))/\mathbb{C}(X(1))$  with

$$\text{Gal}(\mathbb{C}(X(N))/L) = \{\sigma_1 = \text{Id}, \sigma_2, \dots, \sigma_n\}.$$

Then it follows from Proposition 3.1 that  $g(\tau)$  generates  $\mathbb{C}(X(N))$  over  $L$ . Consider the  $n \times n$  matrix

$$B = \left[ g_j^{\sigma_i} \right]_{1 \leq i, j \leq n} \quad \text{where } g_j = g(\tau)^{\sigma_j}.$$

As in Theorem 3.2 it suffices to show  $\det(B) \neq 0$  in order to prove that  $\{g_1, g_2, \dots, g_n\}$  is linearly independent over  $L$ . We derive that

$$\begin{aligned} |\det(B)(r\mathbf{i})| &= \left| \sum_{j_1 j_2 \dots j_n \in S_n} \text{sgn}(j_1 j_2 \dots j_n) g_{j_1}^{\sigma_1}(r\mathbf{i}) g_{j_2}^{\sigma_2}(r\mathbf{i}) \dots g_{j_n}^{\sigma_n}(r\mathbf{i}) \right| \\ &= \left| \pm g(r\mathbf{i})^n + \sum_{\substack{j_1 j_2 \dots j_n \in S_n \text{ such that} \\ \sigma_{j_1} \sigma_{j_2} \dots \sigma_{j_n} \neq \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_n^{-1}}} \pm g^{\sigma_{j_1} \sigma_1}(r\mathbf{i}) g^{\sigma_{j_2} \sigma_2}(r\mathbf{i}) \dots g^{\sigma_{j_n} \sigma_n}(r\mathbf{i}) \right| \\ &\geq |g(r\mathbf{i})|^n \left( 1 - \sum_{\substack{j_1 j_2 \dots j_n \in S_n \text{ such that} \\ \sigma_{j_1} \sigma_{j_2} \dots \sigma_{j_n} \neq \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_n^{-1}}} \left| \frac{g^{\sigma_{j_1} \sigma_1}(r\mathbf{i})}{g(r\mathbf{i})} \right| \left| \frac{g^{\sigma_{j_2} \sigma_2}(r\mathbf{i})}{g(r\mathbf{i})} \right| \dots \left| \frac{g^{\sigma_{j_n} \sigma_n}(r\mathbf{i})}{g(r\mathbf{i})} \right| \right) \\ &\geq |g(r\mathbf{i})|^n \left( 1 - \sum_{\substack{j_1 j_2 \dots j_n \in S_n \text{ such that} \\ \sigma_{j_1} \sigma_{j_2} \dots \sigma_{j_n} \neq \sigma_1^{-1} \sigma_2^{-1} \dots \sigma_n^{-1}}} \frac{1}{d! - 1} \right) \\ &\quad \text{by the fact } \sigma_{j_i} \sigma_i \neq \text{Id for some } 1 \leq i \leq n \text{ and (6)} \\ &> |g(r\mathbf{i})|^n \left( 1 - \frac{n! - 1}{d! - 1} \right) \\ &\geq 0, \end{aligned}$$

which claims  $\det(B) \neq 0$ . Therefore,  $g(\tau)$  is completely free in  $\mathbb{C}(X(N))/\mathbb{C}(X(1))$ , as desired.  $\square$

## References

- [1] D. Bessenohl and K. Johnsen, *Eine Verschärfung des Satzes von der Normalbasis*, J. Algebra 103 (1986), no. 1, 141-159.

- [2] D. Hachenberger, *Universal normal bases for the abelian closure of the field of rational numbers*, Acta Arith. 93 (2000), no. 4, 329-341.
- [3] H. Y. Jung, J. K. Koo and D. H. Shin, *Normal bases of ray class fields over imaginary quadratic fields*, Math. Z. 271 (2012), no. 1-2, 109-116.
- [4] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer-Verlag, New York-Berlin, 1981.
- [5] J. K. Koo and D. H. Shin, *Completely normal elements in some finite abelian extensions*, Cent. Eur. J. Math. 11 (2013), no. 10, 1725-1731.
- [6] S. Lang, *Elliptic Functions*, 2nd edn, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.
- [7] H.-W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. 201 (1959), 119-149.
- [8] T. Okada, *On an extension of a theorem of S. Chowla*, Acta Arith. 38 (1980/81), no. 4, 341-345.
- [9] R. Schertz, *Galoismodulstruktur und elliptische Funktionen*, J. Number Theory 39 (1991), no. 3, 285-326.
- [10] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971.
- [11] M. J. Taylor, *Relative Galois module structure of rings of integers and elliptic functions II*, Ann. of Math. (2) 121 (1985), no. 3, 519-535.
- [12] B. L. van der Waerden, *Algebra I*, Springer, New York, 1991

DEPARTMENT OF MATHEMATICAL SCIENCES  
 KAIST  
 DAEJEON 34141  
 REPUBLIC OF KOREA  
*E-mail address:* jkkoo@math.kaist.ac.kr

DEPARTMENT OF MATHEMATICS  
 HANKUK UNIVERSITY OF FOREIGN STUDIES  
 YONGIN-SI, GYEONGGI-DO 17035  
 REPUBLIC OF KOREA  
*E-mail address:* dhshin@hufs.ac.kr

DEPARTMENT OF MATHEMATICAL SCIENCES  
 KAIST  
 DAEJEON 34141  
 REPUBLIC OF KOREA  
*E-mail address:* math\_dsyoon@kaist.ac.kr